

10/577805

(6)

IAP17 Rec'd PCT/PTO 28 APR 2006

Japanese Patent Laid-open No. HEI 8-322034 A

Publication date : Dec. 3, 1996

Applicant : Matsushita Denki Sangyo K.K.

Title : SCRAMBLING CONTROL METHOD

5

[Conventional art] In order to keep the contents of communication secret in satellite communication, the video/sound signal is transmitted after being scrambled. Thus, only a decoder having viewing/listening rights can view/listen to the communication by descrambling the same. Between analog video signals and digital video signals, digital video signals can be transmitted effectively in a small frequency range by the development of image coding techniques.

15 [0003] Fig. 3 is a schematic diagram of the digital video signal based on the MPEG (Moving Picture Experts Group) standards ISO 11172 and 13818. The digital video signal in this schematic diagram is a layered structure including six layers, that is, a video sequence layer, a
20 GOP (Group Of Picture) layer, a picture layer, a slice layer, a macro block layer, and a block layer. Among these six layers, the top three layers of the layered structure, namely, the video sequence layer, the GOP layer, and the picture layer are shown.

25 [0004] The video sequence layer includes at least one GOP layer. The sequence header before each GOP layer has been omitted in the diagram. The GOP layer, which includes multiple pictures from I pictures, P pictures, and B pictures as image types corresponding to a predictive
30 coding method, usually includes 15 or 12 pictures. At the head is set an I picture, which becomes the reference of the standard. The I picture is a picture for completely encoding within the picture. The P picture is a picture

that carries out prediction from the previous picture(s). The B picture is a picture that carries out prediction from the previous and following pictures. 1 second of video images includes 30 pictures. 1 GOP is the smallest unit for decompressing a video signal and the first complete video image can be displayed by all of the data from the beginning to the end of the GOP being aligned. A video signal image cannot be displayed by only data partway through the GOP.

10 [0005] Fig. 4 is a schematic diagram of the transmission method for the digital video signal based on the MPEG mentioned above. This transmission method has been standardized by international standards (ISO 13818-1) as MPEG systems. Each GOP unit in the GOP layer of Fig. 3 in
15 the digital video signal is transmitted by multiple packets called transport packets (1) to (n) (hereinafter, "TS packet") having 184 bytes. Each TS packet is a fixed-length packet with a 4-byte header and a total of 188 bytes.

20 [0006] A conventional scrambling control method will be explained with reference to the timing chart in Fig. 2. In Fig. 2, line a indicates time. Lines b, c, d, e, and f are common times. Line b indicates a state when a digital signal of GOP units is transmitted by being divided into TS
25 packet units. For ease of explanation, a number has been allocated to each GOP and TS packet. A part of GOP0, GOP1, GOP2, GOP3 and a part of GOP4 are shown. The state when the three GOPs of GOP1, GOP2, and GOP3 are transmitted by being divided into n TS packets including TS1 to TSn is shown. TS1 to TSn, the TS packets of GOP2, are transmitted in order between the times t4 and t6. TS1 to TSn, the TS packets of GOP3 are transmitted in order from time t6.
30 [0007] Line c indicates a state on the transmission side

when a digital signal is scrambled while updating scramble keys Ks1, Ks2, ... for each updating period T1. In an updating period T1 from the times t1 to t5, the TS packet to be transmitted is scrambled by the scramble key Ks1 and 5 between the times t5 and t7 the TS packet to be transmitted is scrambled by the scramble key Ks2.

[0008] The updating period T1 of the scramble key is constant and is a short period of a number of seconds. There is no relationship between the timing for updating 10 the scramble key and the GOP. The data transmitted by the first TS packet after updating of the scramble key in most situations becomes data partway through the GOP. In Fig. 2, the state of updating the scramble key from Ks1 to Ks2 in the time t5, which is partway through GOP2 between the 15 times t4 and t6, is shown.

[0009] Line d indicates a timing of distributing the scramble key from the transmission side to the reception side. The transmission side, in parallel with a scrambling process like the one mentioned above, distributes the 20 scramble key Ks2 in advance for a decoder allowing viewing/listening in the time t3, which is between the scrambling of the TS packet to be transmitted between the times t1 and t5, by the scramble key Ks1.

[0010] Line e received this channel a long while ago on 25 the reception side and indicates a state of the decoder of the reception side in the steady state. The decoder in the steady state, by using the scramble key that is distributed in advance from the transmission side, descrambles the TS packets received between the times t1 and t5, in other 30 words, the TS packets of a part of GOP0, the TS packets of GOP1, and the TS packets of a part of GOP2. In parallel with the descrambling process, the scramble key Ks2 is received in advance at the time t3 and the TS packets

received between the times t5 and t7, in other words, the TS packets of a part of GOP2, the TS packets of GOP3, and the Ts packets of GOP4, are descrambled by Ks2.

Accordingly, because all of the TS packets of GOP1 are
5 descrambled by scramble key Ks1, all of the TS packets of
GOP2 are descrambled by descramble keys Ks1 and Ks2, and
all of the packets of GOP3 are descrambled by the scramble
key Ks2, the complete video images of GOP1, GOP2, and GOP3
can be displayed by decompressing the complete video
10 images.

[0011] When the decoder is not in the steady state, as indicated by line f, a decoder that starts reception of a channel from the time t2 by turning on the power of the decoder or changing of the channel will be explained.

15 Directly after reception of the channel has started, the reception decoder does not have the scramble key Ks1. Therefore, the TS packets to be received cannot be descrambled between the times t2 and t5. Therefore, the video images cannot be decompressed and displayed for the
20 GOPs until time t5.

[0012] Even if reception of the channel starts from the time t2, the scramble key Ks2 can only be received at the time t3. Therefore, descrambling of the packet is possible at the time t5. The TS packets descrambled between the
25 times t5 and t6 are TS packets from partway through GOP2. Therefore, the video image of GOP2 cannot be decompressed. The start of decompression of the complete video image is from GOP3, which starts descrambling from the head data in the time t6.

30 [0013] Therefore, from the beginning of reception to when scrambling can begin is the time t2 to t5 and the time T2, which is the time while descrambling can be done but image display is not possible, in other words, the time t5

to t6. The waiting time from when reception starts until image display is the time t5 to t6. The maximum time of T2 is the time of 1 GOP. Therefore, when 1 GOP includes 15 pictures, it becomes 0.5 seconds.

5 [0014]

[Problem to be Solved by the Invention]

In the conventional scrambling method explained above, as indicated by the line f, in the waiting time from when reception starts until image display, at a TS packet level, 10 there is a time T2 in which scrambling can be performed, but image display is not possible. Therefore, there is a problem that the waiting time becomes much longer.

[0015] In consideration of the above problem, an object of the present invention, at the TS packet level, is to 15 eliminate the time in which descrambling can be performed but image display is not possible in the waiting time needed from the start of reception by changing the channel until image display, and to be able to decrease the waiting time.

20 [0016]

[Means to Solve the Problems]

The present invention solves the problem by a control method in which GOP units based on MPEG, which is an international standard in decoding of moving pictures, are 25 divided into multiple transport packets, transport packets are transported after each has been scrambled by a scramble key, and the scramble keys are updated from the time of transmitting a transport packet including head data of GOP units. In this situation, at the reception side, by the 30 transmission side distributing the scramble keys mentioned above to the reception side in advance, when reception starts partway through the GOP units, by scramble keys distributed in advance from the transmission side,

descrambling from the transport packet including head data of a next GOP unit can be performed and decompression of the corresponding GOP unit is possible.

[0017]

5 [Operation] By the control method mentioned above, the present invention can update the scramble key from the transmission time of the transport packet including the head data of GOP units. Therefore, at the reception side, when reception starts partway through GOP units transmitted
10 from the transmission side, descrambling can be performed from the head data of the transport packet of the next GOP unit. Therefore, decompression of a complete video signal can start by the decompression of this GOP unit, and the waiting time from the start of reception can be decreased.

15

[Fig. 1] A timing chart of a scrambling control method according to an embodiment of the present invention.

[Fig. 2] A timing chart of a conventional scrambling control method.

20

Fig. 1, 2

(Time axis)

(GOP and TS packet)

(Used scramble key)

25 (Scramble key distribution)

(Steady state decoder)

(Reception starting decoder)

TS packets transmitted during this period are scrambled by

30 Ks1

TS packets transmitted during this period are scrambled by

Ks2

Distribution of Ks2

Distribution of Ks3

TS packets received during this period are descrambled by

5 Ks1

TS packets received during this period are descrambled by

Ks2

Reception of Ks2

10 Reception of Ks3

Decompression of GOP0

Decompression of GOP1

Decompression of GOP2

15 Decompression of GOP3

Decompression of GOP4

Descrambling of TS packets is not possible

20 Start of reception

(図2 GOP2は復元不可)

Decompression of GOP2 is not possible

25 Waiting time

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-322034

(43)公開日 平成8年(1996)12月3日

(51) Int.Cl. ⁶	識別記号	序内整理番号	F I	技術表示箇所
H 04 N 7/167			H 04 N 7/167	Z
H 03 M 7/00		9382-5K	H 03 M 7/00	
H 04 K 1/00			H 04 K 1/00	
H 04 L 9/00			H 04 L 9/00	Z
9/10			H 04 N 7/13	Z

審査請求 未請求 請求項の数 2 O L (全 7 頁) 最終頁に統く

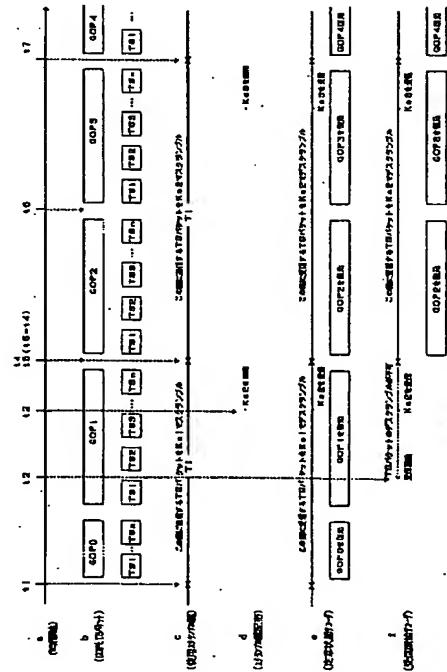
(21)出願番号	特願平7-128121	(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成7年(1995)5月26日	(72)発明者	井上 哲也 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
		(72)発明者	村上 弘規 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
		(72)発明者	勝田 昇 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
		(74)代理人	弁理士 岡田 和秀

(54)【発明の名称】 スクランブル制御方法

(57)【要約】

【目的】MPEG標準に準拠したデジタル映像信号をトランスポートパケット単位にスクランブルをかけながら送信する際、デスクランブル開始と同時に映像画像の復元を可能とし、受信開始から画像表示までの待ち時間を短縮する。

【構成】スクランブル鍵を更新するタイミングをGOPの先頭データを含むトランスポートパケットからすることにより、受信開始後にデスクランブル可能となった最初のトランスポートパケットから順次GOPの全体データを得ることができ、映像画像を復元できる。



【特許請求の範囲】

【請求項1】 動画像における符号化の国際標準であるMPEGに準拠したデジタル映像信号におけるGOP単位を複数のトランSPORTパケット単位に分割するとともに、各トランSPORTパケットをスクランブル鍵でスクランブルして送信し、かつ、前記スクランブル鍵を、GOP単位の先頭のデータを含むトランSPORTパケットの送信時間から更新することを特徴とするスクランブル制御方法。

【請求項2】 前記送信側が、受信側に前記スクランブル鍵を事前に配布することによって、受信側が、送信側から事前に配布された前記スクランブル鍵で、GOP単位の途中からの受信開始時には次のGOP単位の先頭のデータを含むトランSPORTパケットからデスクランブルして当該GOP単位の復元が可能であることを特徴とする請求項1記載のスクランブル制御方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、デジタル映像信号にスクランブルをかけて配信するスクランブル制御方法に関するものである。

【0002】

【従来の技術】衛星通信においては、通信内容を秘匿するため、映像・音声信号にスクランブルをかけて送出し、視聴権を有するデコーダのみがスクランブルを解いて視聴している。画像符号化技術の発達により、アナログ映像信号とデジタル映像信号では、デジタル映像信号の方が小さな周波数帯域で効率よく伝送できる。

【0003】図3は、MPEG (Moving Picture Experts Group:動画像圧縮の国際標準) のISO11172, 13818に準拠したデジタル映像信号の概要図である。この概要図におけるデジタル映像信号はビデオシーケンス層、GOP (Group Of Picture) 層、ピクチャ層、スライス層、マクロブロック層、およびブロック層からなる6層からなる階層構造のうち上位層から3つの階層構造であるビデオシーケンス層、GOP層、ピクチャ層が示されている。

【0004】ビデオシーケンス層は1つ以上のGOP層からなる。ここで各GOP層の前にあるシーケンスヘッダの図示は省略されている。GOP層は予測符号化方式に対応した画像タイプとしてIピクチャ、Pピクチャ、Bピクチャからの複数のピクチャでもって通常15個または12個のピクチャからなっており、その先頭には表示の基準となるIピクチャがおかれる。ここで、Iピクチャはピクチャ内で符号化を完結するピクチャであり、Pピクチャは前ピクチャからの予測を行うピクチャであり、Bピクチャは前後ピクチャからの予測を行うピクチャである。1秒間の映像画像は30ピクチャで構成されている。1GOPは映像画像を復元するための最小単位であり、GOPの先頭から最後までの全てのデータが揃

つて初めて完全な映像画像を表示できる。GOPの途中からのデータだけでは映像画像を復元することはできない。

【0005】図4は、前記MPEGに準拠したデジタル映像信号の伝送方法を示す概要図である。この伝送方法についてもMPEGシステムズとして国際標準（ISO 13818-1）で規格化されている。デジタル映像信号における図3のGOP層にある各GOP単位はそれが184バイト単位の複数のトランSPORTパケット

10 (1)～(n)（以下TSパケット）と呼ばれるパケットで伝送される。TSパケットそれぞれは、4バイトのヘッダを持ち、総計で188バイトの固定長パケットである。

【0006】図2のタイミングチャートを参照して従来のスクランブル制御方法について説明する。図2において、線表aは時間を示す。線表b, c, d, e, fと共に時間である。線表bは、GOP単位のデジタル信号がTSパケット単位に分割されて伝送されている様子を示す。説明のために各GOPやTSパケットに番号を割

20 当てており、GOP0の一部、GOP1, GOP2, GOP3、およびGOP4の一部が示され、そのうちGOP1, GOP2, GOP3の3つのGOPがそれぞれTS1～TSnからなるn個のTSパケットに分割されて伝送されている様子を示している。GOP2のTSパケットであるTS1～TSnは時間t4からt6の間に順次に伝送され、時間t6からはGOP3のTSパケットであるTS1～TSnが順次に伝送される。

【0007】線表cは、送信側で、更新周期T1毎にスクランブル鍵Ks1, Ks2……を更新しながらデジタル信号にスクランブルをかけている様子を示す。時間t1からt5までの更新周期T1においては、送出するTSパケットに対しスクランブル鍵Ks1で、時間t5からt7までの間においては、送出するTSパケットに対しスクランブル鍵Ks2でスクランブルをかける。

【0008】スクランブル鍵の更新周期T1は一定で、数秒程度の短い周期である。スクランブル鍵を更新するタイミングとGOPとの関係は全く無関係であり、スクランブル鍵更新後の最初のTSパケットが伝送しているデータは、確率的にほとんどの場合は、GOPの途中のデータとなる。図2では時間t4からt6の間のGOP2の途中である時間t5でスクランブル鍵がKs1からKs2に更新された様子を示す。

【0009】線表dは、送信側から受信側にスクランブル鍵を配布するタイミングを示している。送信側は、上記のようなスクランブル処理と並行して、時間t1と時間t5の間に送信するTSパケットをスクランブル鍵Ks1でスクランブルしている間の時間t3のタイミングで視聴を許可するデコーダに対してスクランブル鍵Ks2を事前に配布しておく。

50 【0010】線表eは、受信側ずっと以前からこのチ

チャンネルを受信しており、定常状態にある受信側のデコーダの様子を示している。定常状態にあるデコーダは、送信側から事前に配布されたスクランブル鍵K_s1を使用して、時間t₁からt₅の間に受信するTSパケット、つまりGOP0の一部のTSパケット、GOP1のTSパケット、GOP2の一部のTSパケットについてデスクランブルしている。そのデスクランブル処理と並行して時間t₃にスクランブル鍵K_s2を事前に受取り、時間t₅からt₇の間に受信するTSパケットつまりGOP2の一部のTSパケット、GOP3のTSパケット、GOP4の一部のTSパケットについてはK_s2でデスクランブルする。したがって、GOP1の全てのTSパケットはスクランブル鍵K_s1で、GOP2の全てのTSパケットはスクランブル鍵K_s1とK_s2で、GOP3の全てのTSパケットはスクランブル鍵K_s2でデスクランブルできたため、GOP1とGOP2とGOP3は全てその完全な映像画像を復元して表示することができる。

【0011】これに対して、デコーダが定常状態ではなく、線表fのように、デコーダ電源の投入やチャンネル切り替えなどにより、時間t₂からこのチャンネルの受信を開始したデコーダについて説明する。チャンネル受信開始直後は受信デコーダはスクランブル鍵K_s1を持っていないので、時間t₂からt₅までの間に受信するTSパケットをデスクランブルすることはできないから、時間t₅までのGOPについて映像画像を復元して表示することはできない。

【0012】次に、時間t₂からチャンネルの受信を開始しても時間t₃ではスクランブル鍵K_s2を受信できるから、時間t₅からはTSパケットのデスクランブルが可能となる。この場合、時間t₅からt₆までの間にデスクランブルできたTSパケットはGOP2の途中からのTSパケットであるため、GOP2の映像画像を復元することはできない。結局、完全な映像画像の復元が始まるのは、t₆にその先頭データからデスクランブルを開始するGOP3からとなる。

【0013】そのため、受信開始からデスクランブルが開始できるのは受信開始からTSパケットのデスクランブル不可までの時間t₂～t₅と、デスクランブルできながら画像表示ができなかった時間T₂つまり時間t₅～t₆となり、結局、受信開始から画像表示までの待ち時間はt₂からt₆までの時間であり、また、T₂の最大時間は1GOP分の時間となるから、1GOPが1.5ピクチャからなる場合には、0.5秒にもなる。

【0014】

【発明が解決しようとする課題】上述したように従来のスクランブル制御方法においては、線表fに示したように、受信側ではその受信開始から画像表示までの待ち時間の中にTSパケットレベルではデスクランブルできながら画像表示ができないという時間T₂も含まれてくる

ために、待ち時間がさらに長くなるという課題を有していた。

【0015】そこで、本発明は、上述に鑑み、チャンネル切り替えなどによる受信開始から画像表示までに要する待ち時間のうち、TSパケットレベルではデスクランブルできながら画像表示ができないという時間をなくし、待ち時間を短縮できるようにすることを解決すべき課題としている。

【0016】

【課題を解決するための手段】本発明は、動画像における符号化の国際標準であるMPEGに準拠したデジタル映像信号におけるGOP単位を複数のトランスポートパケット単位に分割するとともに、各トランスポートパケットをスクランブル鍵でスクランブルして送信し、かつ、前記スクランブル鍵を、GOP単位の先頭のデータを含むトランスポートパケットの送信時間から更新することを特徴とした制御方法によって前記課題を解決している。この場合、前記送信側が、受信側に前記スクランブル鍵を事前に配布することによって、受信側では、送信側から事前に配布された前記スクランブル鍵で、GOP単位の途中からの受信開始時には次のGOP単位の先頭のデータを含むトランスポートパケットからデスクランブルして当該GOP単位の復元が可能である。

【0017】

【作用】本発明は前記した制御方法により、スクランブル鍵をGOP単位の先頭のデータを含むトランスポートパケットの送信時間から更新するようにしたから、受信側では送信側から送信してきたGOP単位を途中から受信を開始した場合には、次のGOP単位のトランスポートパケットの先頭のデータからデスクランブルできるから、当該GOP単位を復元して完全な映像画像の復元を始めることができ、受信開始からの待ち時間が短縮される。

【0018】

【実施例】以下、図1を参照して本発明の実施例におけるスクランブル制御方法について説明する。図1において、図2と対応する部分についての詳しい説明は省略する。

【0019】

線表bで示すように送信側から各GOP₀、GOP₁、GOP₂、GOP₃、GOP₄それぞれのTSパケットが伝送されている。線表cで示すように送信側では、更新周期T₁毎にスクランブル鍵K_s1、K_s2を更新しながら各更新周期T₁内に伝送するTSパケットのデジタル信号にスクランブルをかけている。つまり時間t₁からt₅の間に送出するTSパケットに対してはスクランブル鍵K_s1で、時間t₅からt₇の間に送出するTSパケットに対してはスクランブル鍵K_s2でスクランブルをかけている。スクランブルの方法には、スクランブル鍵を初期値とするPN乱数系列を信号に足し込む方法とか、スクランブル鍵を暗号鍵として

D E Sのようなブロック暗号を施す方法などがある。スクランブル鍵の更新周期T 1は一定の数秒程度の短い周期である。スクランブル鍵を更新するタイミングt 1, t 5, t 7は、G O Pの先頭データを含むT Sパケットからとする。ここで、t 4 = t 5とし、ちょうどG O P 2の先頭でスクランブル鍵がK s 1からK s 2に更新された様子を示している。線表dは、送信側から受信側にスクランブル鍵を配布するタイミングを示す。

【0020】送信側は、上述したようなスクランブル処理と並行して、時間t 3に視聴を許可するデコーダに対してスクランブル鍵K s 2を事前に受信側に配布しておく。スクランブル鍵の送信は、例えばデジタル映像信号に多重する形で電波で送る。スクランブル鍵の更新周期T 1が十分長い場合には、K s 2を複数回送るようにしてもよい。

【0021】線表eは、受信側においてずっと以前からこのチャンネルを受信しており、定常状態にあるデコーダの様子を示している。定常状態にある受信側デコーダは、時間t 1からt 5の間においては送信側から事前に配布されているスクランブル鍵K s 1を使用して、時間t 1からt 5の間に受信するT Sパケットをデスクランブルしている。そのデスクランブル処理と並行して時間t 3にスクランブル鍵K s 2を事前に受取り、時間t 5からt 7の間に受信するT Sパケットについてはスクランブル鍵K s 2でデスクランブルする。したがって、G O P 2は先頭のデータからの全てのT Sパケットをデスクランブルできたため、その完全な映像画像を復元して表示することができるようになる。

【0022】線表fは、デコーダ電源の投入やチャンネル切り替えなどにより、時間t 2からこのチャンネルの受信を開始した場合の受信側のデコーダの様子を示している(t 1 < t 2 < t 3)。受信開始直後は受信側のデコーダはスクランブル鍵K s 1を受け取っていないか

ら、時間t 2からt 5までの間に受信するT Sパケットをデスクランブルすることはできない。時間t 3にスクランブル鍵K s 2を受け取ってからは、そのスクランブル鍵K s 2でもって時間t 5以降に受信するT Sパケットのデスクランブルが可能となる。デスクランブルを始めた最初のT SパケットにはG O P 2の先頭データが含まれており、G O P 2のT Sパケットが全てデスクランブルされるため、G O P 2から完全な映像画像の復元が始まる。したがって、受信開始から画像表示までの待ち時間は時間t 2からt 5までの間となり、T Sパケットのデスクランブルができなかった時間だけとなる。

【0023】以上のようにこの実施例によれば、スクランブル鍵を更新するタイミングをG O Pの先頭データを含むT Sパケットに合わせたことにより、T Sパケットレベルではデスクランブルできておりながら映像画像の復元ができないといった待ち時間は存在しない。

【0024】

【発明の効果】以上説明したように、本発明によれば、T Sパケットレベルではデスクランブルできておりながら映像画像の復元ができないといった時間をなくすことができるから、デコーダの電源投入やチャンネル切り替えなどによる受信開始から画像表示までに要する待ち時間を短縮することができ、その実用的効果は大きい。

【図面の簡単な説明】

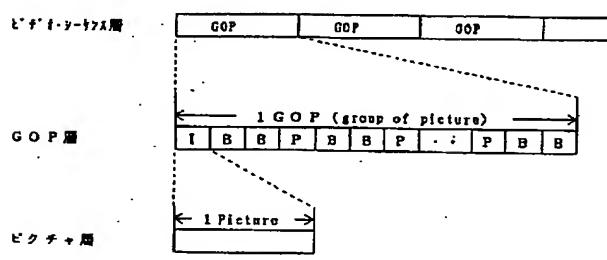
【図1】本発明の実施例におけるスクランブル制御方法のタイミングチャートである。

【図2】従来のスクランブル制御方法のタイミングチャートである。

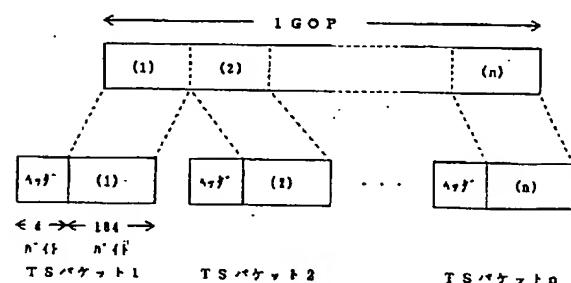
【図3】M P E Gに準拠したデジタル映像信号の概要図である。

【図4】M P E Gに準拠したデジタル映像信号の伝送方法を示す概要図である。

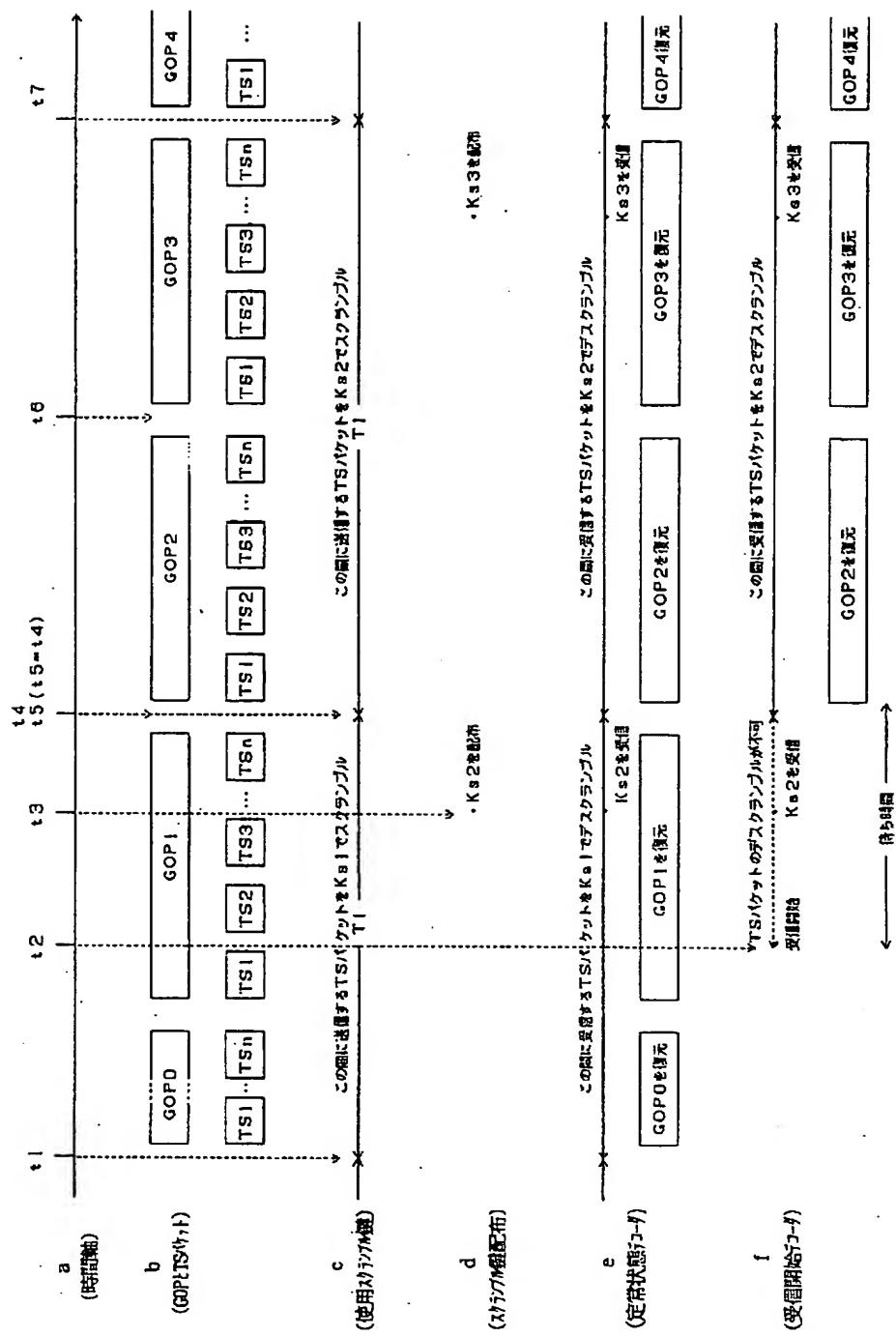
【図3】



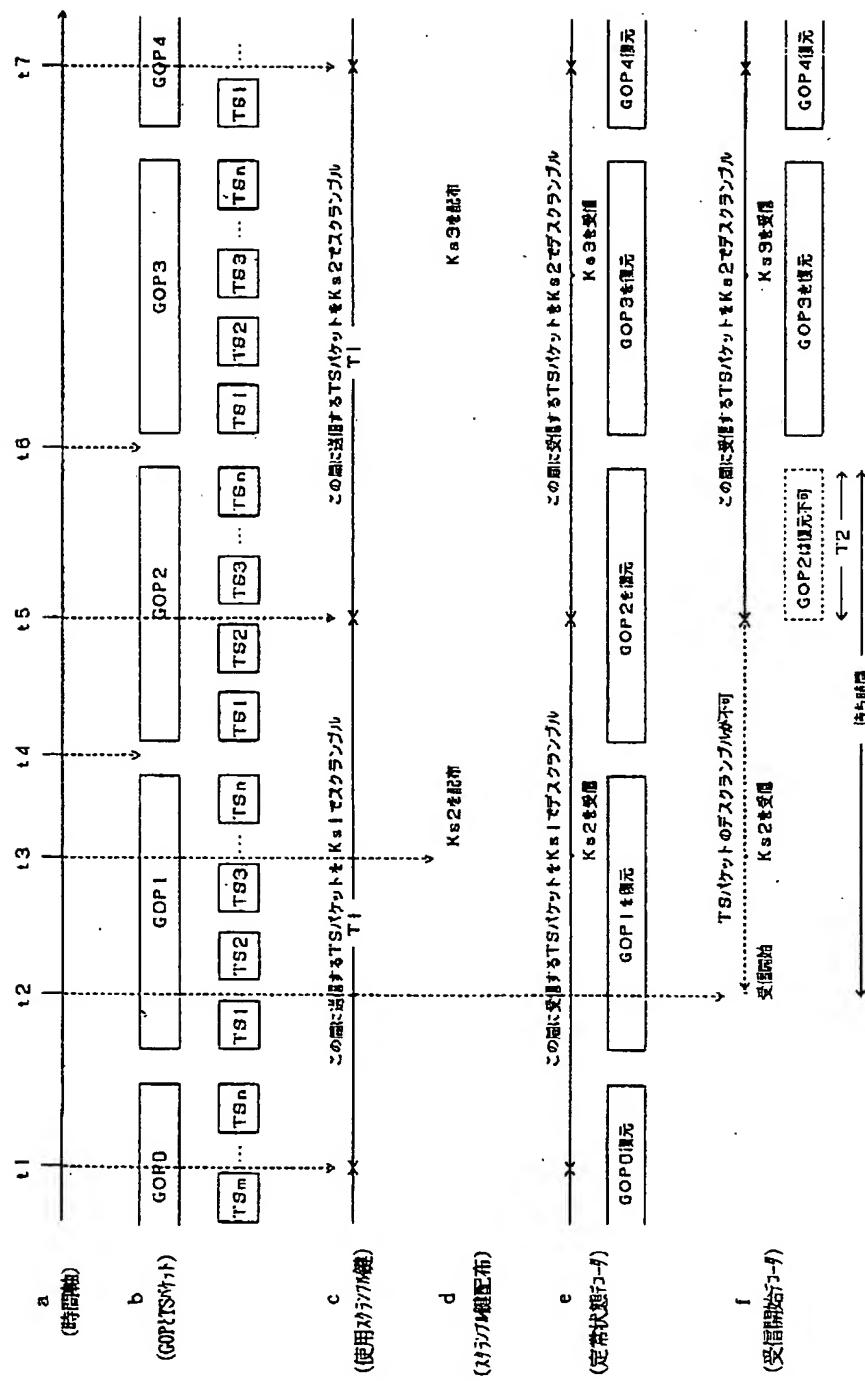
【図4】



【図1】



【図2】



フロントページの続き

(51) Int. Cl. ⁶	識別記号	序内整理番号	F I	技術表示箇所
H 04 L	9/12			
H 04 N	7/24			